REMARKS

This Amendment is fully responsive to the final Office Action dated May 27, 2009, issued in connection with the above-identified application. Claims 1-15, 18-21 and 24 are pending in the present application. With this Amendment, claims 1, 4, 5, 10, 18, 20 and 21 have been amended; and claims 2, 3 and 24 have been canceled without prejudice or disclaimer to the subject matter therein. No new matter has been introduced by the amendments made to the claims. Favorable reconsideration is respectfully requested.

I. Discussion with Examiner

At the outset, the Applicants thank Examiner Nguyen for contacting the Applicants' representative by telephone on May 15, 2009 in order to discuss possible claim amendment to help further distinguish the present invention from the cited prior art. Claim amendments to address the claim objection and the rejection under 35 U.S.C. 101 were also discussed.

Specifically, first, the Examiner suggested including the limitations of dependent claim 9 into independent claims 1, 18, 20 and 21. The Examiner also suggested incorporating the limitations of dependent claim 24 into independent claim 10, and canceling claim 24.

Second, the Examiner suggested further amending claim 20 to address the rejection under 35 U.S.C. 101. Specifically, a recent Supreme Court precedent (i.e., in re Bilski) requires that any process or method must be: 1) tied to a particular apparatus or machine; or 2) transform the underlying subject matter into a different state or thing. Accordingly, the Examiner suggested amending claim 20 to point out the structure used to perform the "candidate calculation step" and the "primality testing step" recited in the claim. It was agreed that it would be sufficient to add a limitation at the end of claim 20 that recites the following:

"wherein the candidate calculation step and the primality testing step are performed by a program stored on a computer-readable medium that when executed by at least one processor causes the prime calculation apparatus to perform the candidate calculation step and the primality testing step."

It was also agreed that support for the above claim amendment can be found at least in ¶[0050]-¶[0052] of the Applicants' disclosure.

II. Allowable Subject Matter

In the Office Action, the Examiner indicates that independent claim 10 would be allowable if amended to address the claim objection noted in the Office Action. Additionally, the Examiner indicates that claims 11-15 would also be allowable by virtue of their dependencies from independent claim 10. The Applicants have amended independent claim 10 to address the claim objection in the Office Action. Accordingly, claims 10-15 should now be allowable over the prior art of record.

III. Claim Objection

In the Office Action, claims 10, 14, 18, 20 and 21 have been objected to because of minor informalities. The Applicants have amended claims 10 and 21 to address the minor informalities noted by the Examiner. Additionally, claim 14, 18 and 20 were amended in the previous response, and the Examiner did not indicate any specific issues with regard to claims 14, 18 and 20 in the Office Action. Accordingly, no amendments are believed to be necessary for claims 14, 18 and 20. Finally, claim 24 has been canceled thereby rending any claim objection to that claim moot (mentioned in item 4, but not specifically listed as objected to). Withdrawal of the objection to claims 10, 14, 18, 20 and 21 is now respectfully requested.

IV. Rejection under 35 U.S.C. 101

In the Office Action, claim 20 has been rejected under 35 U.S.C. 101 for failing to fall within one of the four enumerated statutory classes of patentable subject matter. Specifically, the Examiner indicates that the method recited in the claim must: 1) be tied to a particular machine; or 2) transform underlying subject matter to a different state or thing. Claim 20 has been amended to be consistent with the Examiner's suggestion made during the telephone conversation on May 15, 2009. Withdrawal of the rejection to claim 20 under 35 U.S.C. 101 is now respectfully requested.

V. Rejections Under 35 U.S.C. 103

In the Office Action, claims 1-9, 18, 20, 21 and 24 have been rejected under 35 U.S.C. 103(a) as being unpatentable over the Applicants Admitted Prior Art ("the AAPA") in view of Peyravian et al. (Article entitled "Generation of RSA Keys That Are Guaranteed to be Unique for

Each User," hereafter "Peyravian"). Claims 2, 3 and 24 have been canceled thereby rendering the above rejection to those claims moot. Additionally, the Applicants have amended independent claims 1, 18, 20 and 21 to help further distinguish the present invention from the cited prior art.

For example, independent claim 1 (as amended) recites the following features:

"[a] prime calculating apparatus for calculating a prime candidate N larger than a known prime q and testing primality of the calculated prime candidate N, comprising:

a prime storage unit storing the known prime q;

a management information storage unit storing unique management information;

a random information generation unit operable to read the unique management information from the management information storage unit, and generate random information R based on the read unique management information;

a candidate calculation unit operable to read the prime q from the prime storage unit, and calculate the prime candidate N using the read prime q and the generated random information R, according to N = 2 × random information R × prime q + 1;

a primality testing unit operable to test primality of the calculated prime candidate N according to the Pocklington's primality test; and

an output unit operable to output the calculated prime candidate N as a prime N when the primality of the calculated prime candidate N is determined,

wherein said random information generation unit further includes:

a reading subunit operable to read the unique management information from the management information storage unit;

a random number calculation subunit operable to calculate a random number r;

a combining subunit operable to make a combination of the read unique management information and the generated random number r; and

a computation subunit operable to compute the random information R based on the combination, and

wherein the computation subunit computes the random information R by applying

an injection function to the combination."

The above features of independent claim 1 are similarly recited in independent claims 18, 20 and 21 (as amended). As amended, claims 1, 18, 20 and 21 include the features of dependent claims 2 and 3. Accordingly, the features noted above are fully supported by the Applicants' disclosure.

In the Office Action, the Examiner relies on the AAPA in view of Peyravian for disclosing or suggesting all the features recited in independent claims 1, 18, 20 and 21. However, the Applicants assert that the AAPA in view of Peyravian does not disclose or suggest the features recited in independent claims 1, 18, 20 and 21 (as amended).

First, the Examiner concedes that the AAPA does not explicitly teach a random number R that is generated based on unique management information, and accordingly relies on Peyravian for disclosing or suggesting this feature (see e.g., pg. 2, and lines 3 to 11, page 5 of the Office Action).

However, the Applicants assert that Peyravian mainly discloses that primes p and q (having a random n-bit that are specific to a user) are generated using user-specific data. A random number space having an n-bit is divided into sub-spaces based on unique user-specific data having a b-bit, and the sub-spaces are allocated to specified users respectively. Then, primes p and q are selected from the sub-spaces (see e.g., line 10 from the bottom, right column, page 284 to line 5, left column, page 285). As an example of selecting the primes p and q, the following is taken: ANSI Standard x9.31-1998, Digital signatures using reversible public key cryptography for the financial services industry (rDSA).

Based on the above discussion of Peyravian, the Applicants assert that maintaining the rejection to the present invention (as recited in independent claims 1, 18, 20 and 21) in view of Peyravian is improper for at least the reasons noted below.

First, a proposed modification to a prior art reference (to arrive at the present invention) cannot render the prior art reference unsatisfactory for its intended purpose (MPEP 2143.01(v)).

If a prime candidate N=2xRxq+ I of the present invention is calculated using information obtained based on the method of Peyravian as R, high security cannot be achieved (the scope

might be revealed to an attacker). This is because the information is not random, and since the use of the information is contrary to the AAPA's aim to ensure the security, Peyravian is unsuitable to render obvious the present invention.

Second, the proposed modification cannot change the principle of operation of a reference (MPEP 2143.01(vi)).

Peyravian discloses that two primes are calculated. If a prime candidate N=2xRxq+ I of the present invention is calculated using a value calculated based on the two primes used as R, the calculation step is redundant. Therefore, Peyravian is unsuitable to render obvious the present invention.

Third, Peyravian fails to disclose the definition of all the elements (injection function), and the present invention (as recited in independent claims 1, 18, 20 and 21) clearly differs in structure from Peyravian.

According to the present invention (as recited in independent claims 1, 18, 20 and 21), random information R is generated by applying an injection function to a combination of read unique management information and a generated random number r.

By applying an injection function to the combination, it is possible to generate random information having uniqueness of the combination and randomness caused by transforming the combination (see paragraph [0021] of the Specification). The injection function is, for example, an encryption function using a key K, that is, a function of outputting a ciphertext encrypted using the key K (see paragraph [0074] of the Specification). No such features are believed to be disclosed or suggested by Peyravian.

Based on the above discussion, no combination of the AAPA and Peyravian would result in, or otherwise render obvious, independent claims 1, 18, 20 and 21 (as amended). Likewise, no combination of the AAPA and Peyravian would result in, or otherwise render obvious, claims 4-9 at least by virtue of their dependencies from independent claim 1.

In the Office Action, claim 19 has been rejected under 35 U.S.C. 103(a) as being unpatentable over the AAPA in view of Peyravian, and further in view of Oka et al. (U.S. Publication No. 2002/0108042, hereafter "Oka").

Claim 19 depends from independent claim 18. As noted above, the AAPA in view of Peyravian fails to disclose or suggest all the features of independent claim 18. Additionally, Oka fails to overcome the deficiencies noted above in the AAPA in view of Peyravian. Accordingly, no combination of the AAPA, Peyravian and Oka would result in, or otherwise render obvious, claim 19 at least by virtue of its dependency from independent claim 18.

VI. Conclusion

In view of the above, reconsideration and allowance of this application are now believed to be in order, and such actions are hereby solicited. If any points remain in issue which the Examiner feels may best be resolved through a personal or telephone interview, the Examiner is kindly requested to contact the undersigned at the telephone number listed below.

Respectfully submitted,

Yuichi FUTA et al.

/Mark D. Pratt/
2009.08.18 16:42:04 -04'00'

By: _____
Mark D. Pratt
Registration No. 45794
Attorney for Applicants

MDP/ats
Washington, D.C. 20005-1503
Telephone (202) 721-8200
Facsimile (202) 721-8250
August 18, 2009